UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No.** 2:23-mj-639
	)	
Digital devices listed in Attachment A that	)	**Magistrate Judge** Deavers
Were obtained from the residence of Tristin	)	
Washington located at 4546 Crystal Ball Drive	)	
in Hilliard, Ohio and are currently in HSI custody.	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Trace Way (Your Affiant), a Special Agent with the Homeland Security Investigations, (HSI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.
2. I am a Special Agent with HSI assigned to the Office of the Assistant Special Agent in Charge, Columbus, Ohio. I am currently assigned to the Central Ohio Human Trafficking Task Force (COHTTF). HSI has employed me since November of 2019. Prior to becoming a Special Agent with HSI, I served as a U.S. Border Patrol Agent for approximately two years and a Customs and Border Protection Officer for approximately four years; having begun my federal law enforcement career in August 2013. As a Special Agent my responsibilities and duties include the investigation and enforcement of federal laws and regulations related to customs and immigration violations, including but not limited to narcotics, financial crimes, fraud, human trafficking, child exploitation, and violations of the Immigration and Nationality Act. During my tenure as a Special Agent, I have participated in State and Federal investigations involving the illegal possession of

firearms and narcotics in conjunction with human trafficking and prostitution, human trafficking, narcotics trafficking, and child sexual abuse material (CSAM).

3. I have participated in the execution of search warrants and arrests related to the above-referenced offenses. I have seized or assisted in seizing contraband and evidence, including currency, narcotics, firearms, and documentary evidence, which includes electronically stored documents. I have received criminal investigative training, including 26 weeks of intensive training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. This training included instruction on the methods used by criminals to violate the laws of the United States and evade detection by law enforcement. I have had formal and on-the-job training in matters involving human trafficking, narcotics trafficking, and CSAM from instructors, supervisors, and colleagues. I have been personally involved in investigations concerning the possession, manufacture, transportation, distribution, and importation of controlled substances, as well as methods used to finance drug transactions. I am knowledgeable in the enforcement of state and federal laws pertaining to narcotics and dangerous drugs.
4. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at FLETC and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

II. PURPOSE OF THE AFFIDAVIT

5. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have not withheld any evidence or information which would negate probable cause. I have set forth only the facts necessary to establish probable cause for a search warrant for the

content of numerous digital devices that were seized from the residence of Tristin Washington, located at 4546 Crystal Ball Drive, Hilliard, OH 43026, all of which are currently held in the custody of Homeland Security Investigations (HSI) (hereinafter referred to as the **SUBJECT DEVICES**).

6. The **SUBJECT DEVICES** to be searched are more particularly described in **Attachment A**, for the items specified in **Attachment B**, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A – the sexual exploitation of a minor, distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entirety of the **SUBJECT DEVICES**, wherein the items specified in **Attachment B** may be found, and to seize all items listed in **Attachment B** as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

7. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
8. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or

advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

9. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
10. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.
11. As it is used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.
12. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture,

[1] The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in

or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

13. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.
14. The term "minor", as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as "any person under the age of eighteen years."
15. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."
16. The term "visual depiction," as used herein, is defined pursuant to T18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
17. The term "computer" is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

---

sexually explicit conduct as referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

18. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
19. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.
20. Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
21. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning

that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

22. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. BACKGROUND REGARDING THE INTERNET AND MOBILE APPLICATIONS

23. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

24. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

25. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including AGIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

26. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

27. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusul to come across USB thumb drives that are as large as 128GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 16 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 32 Gigabytes to 256 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the

crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

28. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses and other information both in computer data format and in written record format.

29. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography, or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

30. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
31. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.
32. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
33. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate

law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in **Attachment B**.

34. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include LiveMe, KIK messenger service, Snapchat, Meet24, and Instagram.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

35. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

    a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

    b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect

the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

36. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

37. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, and 2252A, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:

    a. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in **Attachment B**;

    b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in **Attachment B**;

    c. Surveying various files, directories and the individual files they contain;

d. Opening files in order to determine their contents;

e. Scanning storage areas;

f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and/or

g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

39. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VII. INVESTIGATION AND PROBABLE CAUSE

40. On October 30, 2023, the Target Subject, **Tristin WASHINGTON**, re-entered the United States at the Port of Miami (POM) via Carnival Cruise Ship Sunrise. Upon arriving at primary inspection, **WASHINGTON** was selected for secondary inspection by a U.S. Customs and Border Protection (CBP) officer. At secondary inspection, the CBP officer inspected **WASHINGTON**'s personal property, including an Apple iPhone. **WASHINGTON** made a binding declaration to the CBP officer stating he owned the Apple iPhone and provided the passcode for the device. Pursuant to CBP's border search authority, the CBP officer inspected the device and observed depictions of suspected child sexual abuse material contained within in a social media chat, specifically Snapchat.

41. After CBP noted suspected child sexual abuse material on the device, law enforcement agents in the Miami, Florida HSI office were contacted. Special agents arrived on scene and, pursuant to HSI's border search authority, conducted a manual review of the aforementioned social media chat (herein referred to as the CHAT), which was located on **WASHINGTON**'s Apple iPhone. The CHAT occurred between the user of the device, **WASHINGTON**, and another user, herein referred to as B.G., occurred between on or about the afternoon of October 29, 2023 and the morning of October 30, 2023. Your affiant would note that, based on the context of the CHAT, it appeared that some of the CHAT occurred prior to the afternoon of October 29. 2023, had been deleted.

42. During the CHAT, **WASHINGTON** purchased videos from B.G. by sending B.G. a money transfer. After sending the payment, B.G. sent **WASHINGTON** multiple files of suspected child sexual abuse material depicting a nude minor female, exposing her vagina and /or inserting objects into her vagina.
43. Continuing during the CHAT, **WASHINGTON** and B.G. discussed the sale and price of additional depictions of B.G., including those depicting B.G. involved in sexual activity. **WASHINGTON** then sent B.G. another money transfer and received multiple files from B.G. Those files depicted what appeared to be the same minor female as seen in the first set of child sexual abuse files and B.G. was again naked, exposing her genitals, and or engaging in sexual activity.
44. Eventually during the CHAT with **WASHINGTON**, B.G. indicated to **WASHINGTON** that she was 18-years old. **WASHINGTON** then asked for videos which depicted B.G. when she was younger, indicating that he did not care about B.G.'s age. B.G. responded that she was actually 14-years of age but possessed images / videos of herself of when she was 12 years old. **WASHINGTON** then requested depictions of B.G. when she was 12 years old and further, asked for content depicted B.G. "as young as possible". **WASHINGTON** then sent another money transfer to B.G. and received multiple images from B.G. in response. These files included a photograph depicting the same minor female, B.G., with her legs spread exposing her genitals, and a video file depicting the same minor female, B.G., with her legs spread apart, hitting herself on the vagina with an object.
45. During the CHAT, **WASHINGTON** asked B.G. if she had any videos with other females or with "anyone younger". B.G. responded that she had videos of herself when she was younger.
46. Throughout the remaining CHAT, **WASHINGTON** continued to send B.G. additional money transfers. In return, **WASHINGTON** received multiple files from B.G. depicting what appears to be the same minor female, nude and exposing her genitals to the camera, and/or engaged in sexual activity.
47. On or about October 30, 2023, law enforcement interviewed **WASHINGTON** at CBP Secondary Inspection at POM. Prior to questioning, **WASHINGTON** was advised of his *Miranda* rights, which he stated that he understood and waived both verbally and in writing. **WASHINGTON** stated that he owed the Apple iPhone and was the only person

who utilized the device. **WASHINGTON** stated he provided the CBP Officer with the passcode to the device. **WASHINGTON** stated he engaged in the aforementioned social media chat with B.G., acknowledged that B.G. told him she was a minor, and that he had received child sexual abuse material from her which depicted B.G. engaged in sexual activities or engaged in sexually explicit conduct. **WASHINGTON** further stated he received multiple videos from B.G., paid her for the material, and agreed that B.G. was, in fact, a minor. **WASHINGTON** stated the videos and images of B.G. were saved in the chat on his phone. **WASHINGTON** confirmed he currently resided in Hilliard, Ohio and that he had a laptop device at his residence.[2] At that point, a federal criminal complaint and arrest warrant were issued for **WASHINGTON** in the Southern District of Florida.

48. Further searches via law enforcement databases revealed that HSI received information from Kik Messenger, a peer to peer messaging application, indicating that on or about May 3, 2019, at 20:38 UTC via IP address 99.17.246.125, user "jcalvin975" uploaded a child exploitation image to Kik. Kik also provided information that "jcalvin975" had an associated email address of jcalvin975@gmail.com. A subpoena was sent to AT&T on December 12, 2019, requesting subscriber information for the user assigned IP address 99.17.246.125 on May 3, 2019 at 20:38 UTC. The return revealed the subscriber was Tristan **WASHINGTON** at the address of 7864 Solitude Drive, Westerville, Ohio 43081. The return also included additional subscriber information including the email address and phone number which was listed as washington.tristin@gmail.com and (614) 804-9036 respectively. The image uploaded by user "jcalvin975" to Kik depicted a nude prepubescent minor male sitting between two nude prepubescent minor females on a couch. Each of the minor females have an arm around the minor male, and each of the minor females are touching the minor male's erect penis with one hand.

49. In addition, the National Center for Missing and Exploited Children (NCMEC) created Cybertip #53834722 indicating that user jcalvin975@gmail.com had uploaded two videos to the cloud-storage service Dropbox on or about August 18, 2019. User jcalvin975@gmail.com was also shown to have multiple login IP addresses with

[2] **WASHINGTON** also denied that any child exploitation material would be on that laptop, however, your affiant knows that child sexual exploiters, as outlined throughout the affidavit, often amass a collection and keep the content across numerous devices they utilize.

99.17.246.125 which was the same IP address identified by Kik as noted above. One of the files titled "videos (147).mp4" depicted a nude prepubescent minor female lying on her back on a bed. An adult male is seen with his head between the minor female's legs and is licking her vagina. The adult male is also seen touching the minor female's breast.

50. During the time frame for both the Kik and NCMEC tip received by law enforcement, a query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 99.17.246.125 was registered to AT&T. On February 12, 2020, a subpoena/administrative summons was issued to AT&T regarding the IP address described. A review of the results revealed that the account holder was Tristin **WASHINGTON,** who, at the time, resided at 7864 Solitude Dr., Westerville, OH 43081. The investigation revealed, however, that **WASHINGTON** was no longer residing in Westerville, Ohio and instead has a permanent residence in Hilliard, Ohio at 4546 Crystal Ball Drive.
51. On October 31, 2023, your affiant was able to contact an individual **WASHINGTON** claimed he resided with in Ohio at the time he had been arrested federally as outlined above. Your affiant spoke with this individual over the phone, and he/she confirmed that he/she resided at the address of 4546 Crystal Ball Drive in Hilliard Ohio with **WASHINGTON**.
52. Additionally on October 31, 2023, your affiant spoke to the significant other of **WASHINGTON** who had been traveling with **WASHINGTON** at the time he was arrested in Florida, and he/she also confirmed **WASHINGTON** resides at the Hilliard, Ohio residence.
53. On October 31, 2023, a federal search warrant was obtained for the residence of **WASHINGTHON.** The warrant sought to search for and seize all digital media devices at the location of 4546 Crystal ball Drive in Hilliard, Ohio.
54. The following day, on November 1, 2023, the search warrant was executed at the Hilliard, Ohio address. All of the **SUBJECT DEVICES** listed in **Attachment A** were seized from the residence of Tristin **WASHINGTON** during the execution of the search warrants by law enforcement as described above.
55. Based on the information that had been gathered to date by law enforcement, combined with your affiant's belief that Tristin **WASHINGTON** likely possesses the

characteristics common to individuals with a sexual interest in minors, as described below, your affiant believes that there is probable cause that the **SUBJECT DEVICES** contain evidence of Tristin **WASHINGTON's** child pornography and child exploitation activities.

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

56. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in communicating about and engaging in sexual abuse of children

    a. Those who communicate about and engage in sexual abuse of children and exchange or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.

    b. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

    c. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography sometimes maintain any "hard copies" of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections and communications are often

maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

d. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

57. Based upon the conduct of individuals who have a sexual interest in children and who produce, distribute, and receive child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, that they rarely are able to abstain from child pornography activities for a prolonged period of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media. Your affiant therefore submits that there is probable cause to believe the evidence of the offenses 18 U.S.C. §§ 2251, 2252, and 2252A – the sexual exploitation of a minor, distribution, transmission, receipt, and/or possession of child pornography, will be located in the **SUBJECT DEVICES.**

IX. CONCLUSION

58. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, and 2252A – the sexual exploitation of a minor, distribution, transmission, receipt, and/or possession of child pornography, have been committed and that evidence, fruits and instrumentalities of these offenses will be found within the **SUBJECT DEVICES** listed in **Attachment A**, which is incorporated herein by reference. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT DEVICES** described in **Attachment A**, and the seizure of the items described in **Attachment B**.

Trace Way
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this 14th day of November, 2023.

Elizabeth A. Preston Deavers
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE TO BE SEARCHED

The devices to be searched are the following:

1. A white-faced iPad with a silver back, FCC ID: BCGA1432, serial: F4NK7Z7CF196
2. A black Rexing bodyworn camera
3. A black/orange/silver T-Mobile ZTE device
4. A silver and black Kodak easy share camera, with serial: KCTNU12011949
5. A black HP laptop, serial: CND6498DV8

The items described above were seized from the residence of Tristan Washington at 4546 Crystal Ball Drive in Hilliard, Ohio and are currently being held in the care and custod of Homeland Security Investigations.

This warrant authorizes the forensic examination of the **SUBJECT DEVICES** for the purpose of identifying the electronically stored information described **in Attachment B**.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of violations of 18 U.S.C. §§ 2251, 2252, and 2252A – the sexual exploitation of a minor, distribution, transmission, receipt, and/or possession of child pornography, those violations involving Tristan Washington, including:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, and electronic messages,) pertaining to the production, possession, receipt, or distribution of child pornography.
3. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to digital files, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications related to the sexual abuse or exploitation of minors.

6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service.
7. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all visual depictions of minors, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.
9. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
10. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed, posted, and/or traded;
11. Any Internet or cellular telephone communications (including email, social media, etc.) with minors;
12. Evidence of the utilization of peer-to-peer file sharing programs;
13. Evidence of utilization of user names or aliases, email accounts, social media accounts, and online chat programs, and usernames, passwords, and records related to such accounts;
14. Evidence of software that would allow others to control the **SUBJECT DEVICES**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the

presence or absence of security software designed to detect malicious software and evidence of the lack of such malicious software;

15. Evidence indicating the computer user's state of mind as it relates to the crimes under investigation;
16. Evidence that any of the **SUBJECT DEVICES** were attached to any other digital device or digital storage medium;
17. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICES;**
18. Passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICES**;
19. Records of or information about Internet Protocol addresses used by the **SUBJECT DEVICES;**
20. Records of or information about any Internet activity occurring on the **SUBJECT DEVICES**, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.